O I P E
JUL 1 9 2004
JC42
PATENT & TRADEMARK OFFICE

MPOR-26,491 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Michael F. Malone, Frederick J. Murphy
Serial No.:	10/674,910
Filed:	September 29, 2003
Group:	To Be Assigned
Examiner:	To Be Assigned
For:	FORENSIC COMMUNICATION APPARATUS AND METHOD

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

7/15/04
(Date of Deposit)

Gregory M. Howison
(Name of Person Mailing Document)

(Signature)

7/15/04
(Date of Signature)

Dear Sir:

PETITION TO MAKE SPECIAL UNDER 37 CFR 1.102

Applicants, by their attorney of record, hereby petition the Commissioner to make the above-referenced patent application SPECIAL under C.R.F §1.102. Applicants believe that their invention is of peculiar importance to of the public and the government namely Terrorism.

Enclosed are the following:

Statement signed by Mr. Michael Malone explaining how the invention contributes to Countering Terrorism;

Information Disclosure Statement and SB-08; and

Petition Fee as set forth by under 37 C.F.R. 1.17(i) in the amount of $130.00.

07/20/2004 EABUBAK1 00000055 10674910
01 FC:1460 130.00 OP

In view of the foregoing it is respectfully requested that this Petition be granted

The Commissioner is hereby authorized to charge Deposit Account No. 20-0780/MPOR-26,491 any additional fees associated with this Petition or credit any overpayment.

Respectfully submitted,

HOWISON & ARNOTT, L.L.P.

Gregory M. Howison
Registration No. 30,646

GMH/yoc
P.O. Box 741715
Dallas, Texas 75374-1715
Tel: 972-479-0462
Fax: 972-479-0464
July 14, 2004

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Michael F. Malone, Frederick J. Murphy
Serial No.:	10/674,910
Filed:	September 29, 2003
Group:	To Be Assigned
Examiner:	To Be Assigned
For:	FORENSIC COMMUNICATION APPARATUS AND METHOD

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

7/15/04
(Date of Deposit)

Gregory M. Howison
(Name of Person Mailing Document)

(Signature)

7/15/04
(Date of Signature)

Dear Sir:

STATEMENT OF MICHAEL MALONE EXPLAINING WHY THIS PATENT APPLICATION CONTRIBUTES TO COUNTERING TERRORISM

Applicants present inventive concept is directed to an apparatus is disclosed for recording image or other data in real time. The apparatus includes a capture device for capturing the image or other information. Once captured, a local verification device is operable to indelibly mark the captured image or other information with the date, time, location and information identifying the creator of the data. A transmitter is provided for transmitting the locally verified captured image or other information in real time to a secure storage facility. The capture device is operable, after the locally verified captured image or other information is transmitted to the

secure storage facility, to receive and verify acknowledgment of the receipt of the transmitted locally verified captured image or other information to the storage facility.

One of the central embodiments of the submitted FORENSIC COMMUNICATION APPARATUS AND METHOD patent Application; for which we are now requesting that advanced out of turn for examination be provided, describes an apparatus, methods and means for capturing, securing, encrypting, transmitting digital images(s), video clip(s), text, sound, and other digitized data to a secure remote digital repository for secure, tamper resistant, non-repudiation storage and authorized personnel only retrieval.

With the advent of digital media, it has become increasingly easy to copy, counterfeit, falsify and misuse digital information of all kinds. Digital media can be altered in ways that defy detection and time and date stamps can be easily changed with freely available software tools.

Furthermore, this invention provides for the secure non-repudiation of the source and exact time and location of the captured digital images by permanently embedding non-repudiation Digital Certificates steganographically within the captured images. This inventive embodiment is clearly useful for evidentiary and other purposes.

Within the new world of security sensitivity lies the potential for inadvertent or deliberate dissemination of captured images that pose a threat to the privacy of the individual. Our invention provides a method and means that only authorized personnel can retrieve and decipher the images and attendant data.

This invention is directly related to the United States Homeland Security initiatives relating to counter-terrorism inventions as defined in 18 U.S.C. 2331, as well as law enforcement and commercial applications.

ADDITIONAL INFORMATION

On June 1, 2004, Bloomberg News announced the Department of Homeland Security awarded a 10 year contract worth as much as $10 billion to a group led by Accenture Ltd. to develop a system to help track visitors to the United States. It will help implement a security program to collect and share data on foreigners entering the United States as part of the U. S. -Visit program to protect against terrorism, the department said.

According to sources, this security program will be designed to protect against terrorism by incorporating a person's photograph, fingerprints and other information contained in his or her visa and passport and then wirelessly transmit the information to a secure data repository for digital archiving.

As the Homeland Security rolls out their initiatives for border patrol, personnel clearing United Sates Customs and tracking personnel entering and leaving the United States, security within airports, trains or other public security or other forensic applications, the submitted patent and invention addresses and invents many of these requirements.

By definitively being able to identify the source, exact time, place and date of the original captured image; by securely transmitting and storing said images and attendant data, and by assuring that only authorized personnel can access and decipher the images and data and that the original images and data have not been tampered with our invention clearly has numerous beneficial uses. Given the foregoing, Applicants respectfully request that our application be granted Special Status for Examiner's review and Office Action.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Respectfully submitted,

Michael Malone

OIPE JC42
JUL 1 9 2004
PATENT & TRADEMARK OFFICE

MPOR-26,491 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Michael F. Malone, Frederick J. Murphy

Serial No.: 10/674,910

Filed: September 29, 2003

Group: To Be Assigned

Examiner: To Be Assigned

For: FORENSIC COMMUNICATION APPARATUS AND METHOD

Mail Stop DD
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

7/15/04
(Date of Deposit)

Gregory M. Howison
(Name of Person Mailing Document)

(Signature)

7/15/04
(Date of Signature)

Dear Sir:

INFORMATION DISCLOSURE STATEMENT

In accordance with the requirements of 37 C.F.R. §§ 1.56, 1.97, and 1.98, attached please find a Form PTO SB/08 listing information for consideration by the Office in connection with its examination of the above-captioned patent application. A copy of the non-patent literature document is enclosed herewith.

Applicants request that this information disclosure statement be considered and that a copy of the Form PTO SB/08 be returned to the undersigned indicating the consideration of each document listed.

REMARKS

Applicants submit that no representation is made, and no representation is intended, that more relevant material does not exist, or that the order of presentation of these materials in any way

reflects their relevant pertinence. The listing on the attached Form PTO SB/08 is not intended to constitute an admission of any kind. Specifically, this presentation is not an admission that any of the items listed are properly citable against the above-identified application as prior art. Applicants respectfully submit that their invention is patentable over the documents listed on Form PTO SB/08.

To Applicant's knowledge, this information disclosure statement is being filed before the mailing date of a first Office Action on the merits. Therefore, pursuant to 37 C.F.R. §1.97(b)(3), no fee is believed necessary for its consideration. Please charge any necessary fees or deficiencies in fees necessary for the filing of this paper or credit any overpayment to Deposit Account No. 20-0780/MPOR-26,491 of HOWISON & ARNOTT, L.L.P.

Respectfully submitted,

HOWISON & ARNOTT, L.L.P.
Attorneys for Applicants

Gregory M. Howison
Registration No. 30,646

GMH/yoc

P.O. Box 741715
Dallas, Texas 75374-1715
Tel. (972) 479-0462
Fax. (972) 479-0464
June 29, 2004

Please type a plus sign (+) inside this box → +

PTO/SB/08A (08-00)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	10/674,910
Filing Date	September 29, 2003
First Named Inventor	Michael F. Malone et al.
Group Art Unit	To Be Assigned
Examiner Name	To Be Assigned
Attorney Docket Number	MPOR-26,491

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	U.S. Patent Document Number	Kind Code[2] (if known)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		6,222,985		Miyake	04-24-2001	
		6,741,864		Wilcock , et al.	05-25-2004	
		6,636,158		Bando , et al.	10-21-2003	
		6,525,768		Obradovich	02-25-2003	
		6,720,879		Edwards	04-03-2004	
		6,507,371		Hashimoto , et al.	01-14-2003	
		6,498,586		Pankinaho	12-24-2002	
		6,292,633		Nakagawa	09-18-2001	
		6,198,989		Tankhilevich , et al.	03-06-2001	
		5,768,640		Takahashi , et al.	06-16-1998	
		5,642,285		Woo , et al.	06-24-1997	
		6,560,660		Flanagin	05-06-2003	
		6,526,351		Whitham	02-25-2003	
		6,160,964		Imoto	12-12- 2000	
		20040114042		Paolini, Michael A. ; et al.	06-17-2004	
		20030177094		Needham, Bradford H. ; et al.	09-18-2003	
		6,532,298		Cambier , et al.	03-11-2003	
		6,205,249		Moskowitz	03-20-2001	
		6,185,683		Ginter , et al.	02-06-2001	
		20040103283		Hornak, Zoltan	05-27-2004	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Office[3]	Number[4]	Kind Code[5] (if known)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Unique citation designation number. [2] See attached Kinds of U.S. Patent Documents. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Please type a plus sign (+) inside this box → +

PTO/SB/08A (08-00)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	10/674,910
Filing Date	September 29, 2003
First Named Inventor	Michael F. Malone et al.
Group Art Unit	To Be Assigned
Examiner Name	To Be Assigned
Attorney Docket Number	MPOR-26,491

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	U.S. Patent Document Number	Kind Code[2] (if known)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		20040101138		Revital, Dan ; et al.	05-27-2004	
		20040091111		Levy, Kenneth L. ; et al.	05-13-2004	
		20040073568		Yonaha, Makoto	04-15-2004	
		20040073557		Piccionelli, Gregory A. ; et al.	04-15-2004	
		20040068371		Estep, Randall S.	04-8-2004	
		20040053637		Iida, Takayuki	03-18-2004	
		20040049734		Simske, Steven J.	03-11-2004	
		20040044911		Takada, Masayuki ; et al.	03-04-2004	
		20040039930		Ohmori, Motoji ; et al.	02-26-2004	
		20040032499		Silverbrook, Kia ; et al.	02-19-2004	
		20040023686		King, John J. ; et al.	02-05-2004	
		20040005078		Tillotson, Scott Andrew	01-08-2004	
		20040022444		Rhoads, Geoffrey B.	02-05-2004	
		6,714,778		Nykanen , et al.	03-30-2004	
		6,532,298		Cambier , et al.	03-11-2003	
		6,205,249		Moskowitz	03-20-2001	
		852557		Acosta; Edward	05-07-1997	
		6,424,968		Broster, et al.	07-23-2002	
		194188		Broster; Ian	04-29-1999	
		865826		Sandford, II; Maxwell T.	05-30-1997	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Office[3]	Number[4]	Kind Code[5] (if known)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Unique citation designation number. [2] See attached Kinds of U.S. Patent Documents. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Please type a plus sign (+) inside this box →

PTO/SB/08B (08-00)
Approved for use through 10/31/2002. OMB 0651-0031
U. S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	10/674,910
Filing Date	September 29, 2003
First Named Inventor	Michael F. Malone et al.
Group Art Unit	To Be Assigned
Examiner Name	To Be Assigned
Attorney Docket Number	MPOR-26,491

OTHER PRIOR ART -- NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	1	H. Krawczyk, RFC 2104 (RFC2104) RFC 2104 - HMAC: Keyed-Hashing for Message Authentication http://www.faqs.org/rfcs/rfc2104.htm February 1997,	
	2		
	3		
	4		
	5		
	6		
	7		
	8		
	9		

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Unique citation designation number. [2] Applicant is to place a check mark here if English language Translation is attached.

RFC 2104 (RFC2104)

RFC 2104 - HMAC: Keyed-Hashing for Message Authentication

Network Working Group
Request for Comments: 2104
Category: Informational

H. Krawczyk
IBM
M. Bellare
UCSD
R. Canetti
IBM

February 1997

HMAC: Keyed-Hashing for Message Authentication

Status of This Memo

This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Abstract

This document describes HMAC, a mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function, e.g., MD5, SHA-1, in combination with a secret shared key. The cryptographic strength of HMAC depends on the properties of the underlying hash function.

1. Introduction

Providing a way to check the integrity of information transmitted over or stored in an unreliable medium is a prime necessity in the world of open computing and communications. Mechanisms that provide such integrity check based on a secret key are usually called "message authentication codes" (MAC). Typically, message authentication codes are used between two parties that share a secret

key in order to validate information transmitted between these parties. In this document we present such a MAC mechanism based on cryptographic hash functions. This mechanism, called HMAC, is based on work by the authors [BCK1] where the construction is presented and cryptographically analyzed. We refer to that work for the details on the rationale and security analysis of HMAC, and its comparison to other keyed-hash methods.

HMAC can be used in combination with any iterated cryptographic hash function. MD5 and SHA-1 are examples of such hash functions. HMAC also uses a secret key for calculation and verification of the message authentication values. The main goals behind this construction are

* To use, without modifications, available hash functions. In particular, hash functions that perform well in software, and for which code is freely and widely available.

* To preserve the original performance of the hash function without incurring a significant degradation.

* To use and handle keys in a simple way.

* To have a well understood cryptographic analysis of the strength of the authentication mechanism based on reasonable assumptions on the underlying hash function.

* To allow for easy replaceability of the underlying hash function in case that faster or more secure hash functions are found or required.

This document specifies HMAC using a generic cryptographic hash function (denoted by H). Specific instantiations of HMAC need to define a particular hash function. Current candidates for such hash functions include SHA-1 [SHA], MD5 [MD5], RIPEMD-128/160 [RIPEMD]. These different realizations of HMAC will be denoted by HMAC-SHA1, HMAC-MD5, HMAC-RIPEMD, etc.

Note: To the date of writing of this document MD5 and SHA-1 are the most widely used cryptographic hash functions. MD5 has been recently shown to be vulnerable to collision search attacks [Dobb]. This attack and other currently known weaknesses of MD5 do not compromise the use of MD5 within HMAC as specified in this document (see [Dobb]); however, SHA-1 appears to be a cryptographically stronger function. To this date, MD5 can be considered for use in HMAC for applications where the superior performance of MD5 is critical. In any case, implementers and users need to be aware of possible cryptanalytic developments regarding any of these cryptographic hash functions, and the eventual need to replace the underlying hash function. (See section 6 for more information on the security of HMAC.)

2. Definition of HMAC

The definition of HMAC requires a cryptographic hash function, which we denote by H, and a secret key K. We assume H to be a cryptographic hash function where data is hashed by iterating a basic compression function on blocks of data. We denote by B the byte-length of such blocks (B=64 for all the above mentioned examples of hash functions), and by L the byte-length of hash outputs (L=16 for MD5, L=20 for SHA-1). The authentication key K can be of any length up to B, the block length of the hash function. Applications that use keys longer than B bytes will first hash the key using H and then use the resultant L byte string as the actual key to HMAC. In any case the minimal recommended length for K is L bytes (as the hash output length). See section 3 for more information on keys.

We define two fixed and different strings ipad and opad as follows (the 'i' and 'o' are mnemonics for inner and outer):

```
ipad = the byte 0x36 repeated B times
opad = the byte 0x5C repeated B times.
```

To compute HMAC over the data `text' we perform

```
H(K XOR opad, H(K XOR ipad, text))
```

Namely,

(1) append zeros to the end of K to create a B byte string (e.g., if K is of length 20 bytes and B=64, then K will be appended with 44 zero bytes 0x00)
(2) XOR (bitwise exclusive-OR) the B byte string computed in step (1) with ipad
(3) append the stream of data 'text' to the B byte string resulting from step (2)
(4) apply H to the stream generated in step (3)
(5) XOR (bitwise exclusive-OR) the B byte string computed in step (1) with opad
(6) append the H result from step (4) to the B byte string resulting from step (5)
(7) apply H to the stream generated in step (6) and output the result

For illustration purposes, sample code based on MD5 is provided as an appendix.

3. Keys

The key for HMAC can be of any length (keys longer than B bytes are first hashed using H). However, less than L bytes is strongly discouraged as it would decrease the security strength of the function. Keys longer than L bytes are acceptable but the extra length would not significantly increase the function strength. (A longer key may be advisable if the randomness of the key is considered weak.)

Keys need to be chosen at random (or using a cryptographically strong pseudo-random generator seeded with a random seed), and periodically refreshed. (Current attacks do not indicate a specific recommended frequency for key changes as these attacks are practically infeasible. However, periodic key refreshment is a fundamental security practice that helps against potential weaknesses of the function and keys, and limits the damage of an exposed key.)

4. Implementation Note

HMAC is defined in such a way that the underlying hash function H can be used with no modification to its code. In particular, it uses the function H with the pre-defined initial value IV (a fixed value specified by each iterative hash function to initialize its compression function). However, if desired, a performance improvement can be achieved at the cost of (possibly) modifying the code of H to support variable IVs.

The idea is that the intermediate results of the compression function on the B-byte blocks (K XOR ipad) and (K XOR opad) can be precomputed only once at the time of generation of the key K, or before its first use. These intermediate results are stored and then used to initialize the IV of H each time that a message needs to be authenticated. This method saves, for each authenticated message, the application of the compression function of H on two B-byte blocks (i.e., on (K XOR ipad) and (K XOR opad)). Such a savings may be significant when authenticating short streams of data. We stress that the stored intermediate values need to be treated and protected the same as secret keys.

Choosing to implement HMAC in the above way is a decision of the local implementation and has no effect on inter-operability.

5. Truncated output

A well-known practice with message authentication codes is to truncate the output of the MAC and output only part of the bits (e.g., [MM, ANSI]). Preneel and van Oorschot [PV] show some analytical advantages of truncating the output of hash-based MAC functions. The results in this area are not absolute as for the overall security advantages of truncation. It has advantages (less information on the hash result available to an attacker) and disadvantages (less bits to predict for the attacker). Applications of HMAC can choose to truncate the output of HMAC by outputting the t leftmost bits of the HMAC computation for some parameter t (namely, the computation is carried in the normal way as defined in section 2 above but the end result is truncated to t bits). We recommend that the output length t be not less than half the length of the hash

output (to match the birthday attack bound) and not less than 80 bits (a suitable lower bound on the number of bits that need to be predicted by an attacker). We propose denoting a realization of HMAC that uses a hash function H with t bits of output as HMAC-H-t. For example, HMAC-SHA1-80 denotes HMAC computed using the SHA-1 function and with the output truncated to 80 bits. (If the parameter t is not specified, e.g. HMAC-MD5, then it is assumed that all the bits of the hash are output.)

6. Security

The security of the message authentication mechanism presented here depends on cryptographic properties of the hash function H: the resistance to collision finding (limited to the case where the initial value is secret and random, and where the output of the function is not explicitly available to the attacker), and the message authentication property of the compression function of H when applied to single blocks (in HMAC these blocks are partially unknown to an attacker as they contain the result of the inner H computation and, in particular, cannot be fully chosen by the attacker).

These properties, and actually stronger ones, are commonly assumed for hash functions of the kind used with HMAC. In particular, a hash function for which the above properties do not hold would become unsuitable for most (probably, all) cryptographic applications, including alternative message authentication schemes based on such functions. (For a complete analysis and rationale of the HMAC function the reader is referred to [BCK1].)

Given the limited confidence gained so far as for the cryptographic strength of candidate hash functions, it is important to observe the following two properties of the HMAC construction and its secure use for message authentication:

1. The construction is independent of the details of the particular hash function H in use and then the latter can be replaced by any other secure (iterative) cryptographic hash function.

2. Message authentication, as opposed to encryption, has a "transient" effect. A published breaking of a message authentication scheme would lead to the replacement of that scheme, but would have no adversarial effect on information authenticated in the past. This is in sharp contrast with encryption, where information encrypted today may suffer from exposure in the future if, and when, the encryption algorithm is broken.

The strongest attack known against HMAC is based on the frequency of collisions for the hash function H ("birthday attack") [PV,BCK2], and is totally impractical for minimally reasonable hash functions.

As an example, if we consider a hash function like MD5 where the output length equals L=16 bytes (128 bits) the attacker needs to acquire the correct message authentication tags computed (with the _same_ secret key K!) on about 2**64 known plaintexts. This would require the processing of at least 2**64 blocks under H, an impossible task in any realistic scenario (for a block length of 64 bytes this would take 250,000 years in a continuous 1Gbps link, and without changing the secret key K during all this time). This attack could become realistic only if serious flaws in the collision behavior of the function H are discovered (e.g. collisions found after 2**30 messages). Such a discovery would determine the immediate replacement of the function H (the effects of such failure would be far more severe for the traditional uses of H in the context of digital signatures, public key certificates, etc.).

Note: this attack needs to be strongly contrasted with regular collision attacks on cryptographic hash functions where no secret key is involved and where 2**64 off-line parallelizable (!) operations suffice to find collisions. The latter attack is approaching feasibility [VW] while the birthday attack on HMAC is totally impractical. (In the above examples, if one uses a hash function with, say, 160 bit of output then 2**64 should be replaced by 2**80.)

A correct implementation of the above construction, the choice of random (or cryptographically pseudorandom) keys, a secure key exchange mechanism, frequent key refreshments, and good secrecy protection of keys are all essential ingredients for the security of the integrity verification mechanism provided by HMAC.

Appendix -- Sample Code

For the sake of illustration we provide the following sample code for the implementation of HMAC-MD5 as well as some corresponding test vectors (the code is based on MD5 code as described in [MD5]).

```
/*
** Function: hmac_md5
*/

void
hmac_md5(text, text_len, key, key_len, digest)
unsigned char*  text;                /* pointer to data stream */
int             text_len;            /* length of data stream */
unsigned char*  key;                 /* pointer to authentication key
*/
int             key_len;             /* length of authentication key */
caddr_t         digest;              /* caller digest to be filled in
*/

{
        MD5_CTX context;
        unsigned char k_ipad[65];    /* inner padding -
```

```
                                 * key XORd with ipad
                                 */
unsigned char k_opad[65];       /* outer padding -
                                 * key XORd with opad
                                 */
unsigned char tk[16];
int i;
/* if key is longer than 64 bytes reset it to key=MD5(key) */
if (key_len > 64) {

        MD5_CTX      tctx;

        MD5Init(&tctx);
        MD5Update(&tctx, key, key_len);
        MD5Final(tk, &tctx);

        key = tk;
        key_len = 16;
}

/*
 * the HMAC_MD5 transform looks like:
 *
 * MD5(K XOR opad, MD5(K XOR ipad, text))
 *
 * where K is an n byte key
 * ipad is the byte 0x36 repeated 64 times

 * opad is the byte 0x5c repeated 64 times
 * and text is the data being protected
 */

/* start out by storing key in pads */
bzero( k_ipad, sizeof k_ipad);
bzero( k_opad, sizeof k_opad);
bcopy( key, k_ipad, key_len);
bcopy( key, k_opad, key_len);

/* XOR key with ipad and opad values */
for (i=0; i<64; i++) {
        k_ipad[i] ^= 0x36;
        k_opad[i] ^= 0x5c;
}
/*
 * perform inner MD5
 */
MD5Init(&context);                   /* init context for 1st
                                      * pass */
MD5Update(&context, k_ipad, 64)      /* start with inner pad */
MD5Update(&context, text, text_len); /* then text of datagram
*/
MD5Final(digest, &context);          /* finish up 1st pass */
/*
 * perform outer MD5
 */
MD5Init(&context);                   /* init context for 2nd
                                      * pass */
```

```
        MD5Update(&context, k_opad, 64);     /* start with outer pad */
        MD5Update(&context, digest, 16);     /* then results of 1st
                                              * hash */
        MD5Final(digest, &context);          /* finish up 2nd pass */
}
```

Test Vectors (Trailing '\0' of a character string not included in test):

```
  key =         0x0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b
  key_len =     16 bytes
  data =        "Hi There"
  data_len =    8  bytes
  digest =      0x9294727a3638bb1c13f48ef8158bfc9d

  key =         "Jefe"
  data =        "what do ya want for nothing?"
  data_len =    28 bytes
  digest =      0x750c783e6ab0b503eaa86e310a5db738

  key =         0xAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

  key_len       16 bytes
  data =        0xDDDDDDDDDDDDDDDDDDDD...
                ..DDDDDDDDDDDDDDDDDDDD...
                ..DDDDDDDDDDDDDDDDDDDD...
                ..DDDDDDDDDDDDDDDDDDDD...
                ..DDDDDDDDDDDDDDDDDDDD
  data_len =    50 bytes
  digest =      0x56be34521d144c88dbb8c733f0e8b3f6
```

Acknowledgments

Pau-Chen Cheng, Jeff Kraemer, and Michael Oehler, have provided useful comments on early drafts, and ran the first interoperability tests of this specification. Jeff and Pau-Chen kindly provided the sample code and test vectors that appear in the appendix. Burt Kaliski, Bart Preneel, Matt Robshaw, Adi Shamir, and Paul van Oorschot have provided useful comments and suggestions during the investigation of the HMAC construction.

References

[ANSI] ANSI X9.9, "American National Standard for Financial Institution Message Authentication (Wholesale)," American Bankers Association, 1981. Revised 1986.

[Atk] Atkinson, R., "IP Authentication Header", RFC 1826, August 1995.

[BCK1] M. Bellare, R. Canetti, and H. Krawczyk, "Keyed Hash Functions and Message Authentication", Proceedings of Crypto'96, LNCS 1109, pp. 1-15. (http://www.research.ibm.com/security/keyed-md5.html)

[BCK2] M. Bellare, R. Canetti, and H. Krawczyk,

"Pseudorandom Functions Revisited: The Cascade Construction",
Proceedings of FOCS'96.

[Dobb] H. Dobbertin, "The Status of MD5 After a Recent Attack", RSA Labs' CryptoBytes, Vol. 2 No. 2, Summer 1996. http://www.rsa.com/rsalabs/pubs/cryptobytes.html

[PV] B. Preneel and P. van Oorschot, "Building fast MACs from hash functions", Advances in Cryptology -- CRYPTO'95 Proceedings, Lecture Notes in Computer Science, Springer-Verlag Vol.963, 1995, pp. 1-14.

[MD5] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[MM] Meyer, S. and Matyas, S.M., Cryptography, New York Wiley, 1982.

[RIPEMD] H. Dobbertin, A. Bosselaers, and B. Preneel, "RIPEMD-160: A strengthened version of RIPEMD", Fast Software Encryption, LNCS Vol 1039, pp. 71-82. ftp://ftp.esat.kuleuven.ac.be/pub/COSIC/bosselae/ripemd/.

[SHA] NIST, FIPS PUB 180-1: Secure Hash Standard, April 1995.

[Tsu] G. Tsudik, "Message authentication with one-way hash functions", In Proceedings of Infocom'92, May 1992. (Also in "Access Control and Policy Enforcement in Internetworks", Ph.D. Dissertation, Computer Science Department, University of Southern California, April 1991.)

[VW] P. van Oorschot and M. Wiener, "Parallel Collision Search with Applications to Hash Functions and Discrete Logarithms", Proceedings of the 2nd ACM Conf. Computer and Communications Security, Fairfax, VA, November 1994.

Authors' Addresses

Hugo Krawczyk
IBM T.J. Watson Research Center
P.O.Box 704
Yorktown Heights, NY 10598

EMail: hugo@watson.ibm.com

Mihir Bellare
Dept of Computer Science and Engineering
Mail Code 0114
University of California at San Diego
9500 Gilman Drive
La Jolla, CA 92093

EMail: mihir@cs.ucsd.edu

Ran Canetti

IBM T.J. Watson Research Center
P.O.Box 704
Yorktown Heights, NY 10598

EMail: canetti@watson.ibm.com

Comment on RFC 2104

Previous: RFC 2103 - Mobility Support for Nimrod : Challenges and Solution Approaches

Next: RFC 2105 - Cisco Systems' Tag Switching Architecture Overview

[RFC Index | RFC Search | Usenet FAQs | Web FAQs | Documents | Cities]

O I P E JC42
JUL 1 9 2004
PATENT & TRADEMARK OFFICE

$ 1FW

PTO/SB/21 (08-03)
Approved for use through 08/30/2003. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/674,910
Filing Date	September 29, 2003
First Named Inventor	Michael F. Malone et al.
Art Unit	To Be Assigned
Examiner Name	To Be Assigned
Attorney Docket Number	MPOR-26,491
Total Number of Pages in This Submission	

ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
  - [x] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [x] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Response to Missing Parts/ Incomplete Application
  - [ ] Response to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [x] Petition — Petition to Make Special under CFR 1.102
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) ________
- [ ] After Allowance communication to Technology Center (TC)
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- [ ] Proprietary Information
- [ ] Status Letter
- [x] Other Enclosure(s) (please Identify below):

Post card, One non-patent literature reference,

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	HOWISON & ARNOTT, L.L.P. Gregory M. Howison Reg. 30,646
Signature	[signature]
Date	7/15/04

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Typed or printed name	Gregory M. Howison		
Signature	[signature]	Date	7/15/04

PTO/SB/17 (10-03)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

FEE TRANSMITTAL for FY 2004

Effective 10/01/2003. Patent fees are subject to annual revision.

☑ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 130.00

Complete if Known	
Application Number	10/674,910
Filing Date	September 29, 2003
First Named Inventor	Michael F. Malone et al.
Examiner Name	To Be Assigned
Art Unit	To Be Assigned
Attorney Docket No.	MPOR-26,491

METHOD OF PAYMENT (*check all that apply*)

☑ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☑ Deposit Account:

Deposit Account Number: 20-0780/MPOR-26,491

Deposit Account Name:

The Director is authorized to: *(check all that apply)*

☐ Charge fee(s) indicated below ☑ Credit any overpayments

☑ Charge any additional fee(s) or any underpayment of fee(s)

☐ Charge fee(s) indicated below, **except for the filing fee**

to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	770	2001	385	Utility filing fee	
1002	340	2002	170	Design filing fee	
1003	530	2003	265	Plant filing fee	
1004	770	2004	385	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

SUBTOTAL (1) ($)

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

			Extra Claims		Fee from below		Fee Paid
Total Claims		-20** =		X		=	
Independent Claims		- 3** =		X		=	
Multiple Dependent						=	

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	86	2201	43	Independent claims in excess of 3
1203	290	2203	145	Multiple dependent claim, if not paid
1204	86	2204	43	** Reissue independent claims over original patent
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($)

***or number previously paid, if greater; For Reissues, see above*

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	420	2252	210	Extension for reply within second month	
1253	950	2253	475	Extension for reply within third month	
1254	1,480	2254	740	Extension for reply within fourth month	
1255	2,010	2255	1,005	Extension for reply within fifth month	
1401	330	2401	165	Notice of Appeal	
1402	330	2402	165	Filing a brief in support of an appeal	
1403	290	2403	145	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,330	2453	665	Petition to revive - unintentional	
1501	1,330	2501	665	Utility issue fee (or reissue)	
1502	480	2502	240	Design issue fee	
1503	640	2503	320	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	130.00
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	770	2809	385	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	770	2810	385	For each additional invention to be examined (37 CFR 1.129(b))	
1801	770	2801	385	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) ____________

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($) 130.00

SUBMITTED BY		(Complete *(if applicable)*)	
Name *(Print/Type)*	Gregory M. Howison	Registration No. *(Attorney/Agent)* 30,646	Telephone 972-680-6050
Signature	[signature]		Date 7/15/04

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.